NASA Policy Directive

NPD 1660.1B
Effective Date: November 18, 2008
Expiration Date: November 18, 2013

COMPLIANCE IS MANDATORY

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: NASA Counterintelligence (CI) Policy

Responsible Office: Office of Security and Program Protection

1. POLICY

a. It is NASA policy to establish and maintain a counterintelligence (CI) and counterterrorism (CT) program. This program shall be conducted pursuant to the National Aeronautics and Space Act of 1958, as amended, and in conformance with other applicable laws, Executive Orders, Presidential Decision Directives, Federal Regulations, and NASA Policy Directives.

b. The Office of Security and Program Protection (OSPP) shall manage the NASA CI/CT program. The CI/CT objective is to detect, deter, and neutralize potential threats posed by foreign intelligence services (FIS), other foreign entities, and acts of terrorism to include trusted insiders who would engage in activities on behalf of an FIS or terrorist entity.

c. The OSPP shall utilize information and undertake approved NASA CI/CT activities to protect the Agency against espionage; sabotage; other intelligence activities; terrorism; or threats conducted for or on behalf of persons, organizations, or foreign powers that are directed toward NASA Federal and contract employees, facilities, operations, and information to include the Arms Export Controlled Act, NASA privileged/proprietary, sensitive but unclassified (SBU), and classified national security information (CNSI).

2. APPLICABILITY

a. This NPD is applicable to all NASA Federal employees, programs, projects, operations, and other activities conducted by or for NASA Headquarters (HQ) and NASA Centers, including Component Facilities and Technical Service Support Centers, and to contractor personnel or other persons or entity to the extent provided in the contract or other governing instrument.

b. Nothing in this directive shall be construed as limiting the authorities of the Inspector General under the Inspector General Act of 1978, as amended.

c. For purposes of this directive "counterintelligence and counterterrorism" means, but is not limited to, information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of persons, organizations, foreign powers, or terrorist activities. "NASA counterintelligence and counterterrorism inquiry or investigation" means, but is not limited to, limited gathering and examination of information or allegation indicating that NASA employees or contractors, information, or resources may be or have been involved with, or targeted by, agents of a foreign power or terrorist group.

3. AUTHORITY

a. 42 U.S.C. 2473 (c), Section 203 (c) of the National Aeronautics and Space Act of 1958, as amended.

b. 42 U.S.C. 2455, Section 304 of the National Aeronautics and Space Act of 1958, as amended. c. NPR 1000.3C, The NASA Organization.

4. REFERENCES

a. 5 U.S.C. Section 552a, The Privacy Act of 1974 (Public Law 93-579), as amended.

b. 5 U.S.C. App., Inspector General Act of 1978, as amended.

c. 18 U.S.C. Sections 1831-1839, Title I of the Economic Espionage Act of 1996 (Public Law 104-294), as amended (as related to CI/CT).

d. 50 U.S.C. 401a, Section 3 of the National Security Act of 1947, as amended.

e. 50 U.S.C. 402a, Section 811 of the Intelligence Authorization Act for Fiscal Year 1995 (Public Law 103-359), as amended.

f. Executive Order 10450, Security Requirements for Government Employees, April 27, 1953, reprinted as amended (3 CFR 1949 - 1953 Compilation).

g. Executive Order 12333, United States Intelligence Activities, (December 4, 1981,) reprinted as amended (3 CFR 1981 Compilation).

h. Executive Order 12958, Classified National Security Information, (April 17, 1995,) reprinted as amended (3 CFR 1995 Compilation).

i. Executive Order 12968, Access to Classified Information, August 2, 1995, reprinted as amended (3 CFR 1995 Compilation).

j. Presidential Decision Directive 39, Counterterrorism Policy, June 21, 1995, as amended.

k. Presidential Decision Directive 62, Protection Against Unconventional Threats to the Homeland and Americans Overseas, May 22, 1998, as amended.

l. Presidential Decision Directive 63, Critical Infrastructure Protection, May 22, 1998, as amended.

m. NPR 1660.1, CI/CT Procedural Requirements.

n. NPR 2810.1A, Security of Information Technology.

o. Memorandum of Understanding between the Federal Bureau of Investigation (FBI) and NASA, dated December 12, 2002.

p. NPR 1441.1D, NASA Records Retention Schedules.

5. RESPONSIBILITY

a. The Assistant Administrator for OSPP has the responsibility for overall policy, direction, and oversight for the NASA CI/CT program. The Assistant Administrator has designated the OSPP CI/CT Program Director as having the overall responsibility to manage and administer the NASA CI/CT program to include prioritizing program objectives, identifying resources, training, equipment needs, and direct supervision of its special agents assigned to HQ and Centers CI/CT offices. The NASA CI/CT Program Director's primary responsibilities include the following:

(1) Establish CI/CT policy and procedures and disseminate that information to HQ and Center CI/CT special agents.

(2) Act as liaison with the U.S. intelligence community on matters concerning foreign intelligence and terrorism matters directed toward NASA Federal and contract employees, information, and resources. This responsibility focuses on the utilization and dissemination of CI/CT threat information. HQ and Center CI/CT offices shall receive information from the CI/CT Program Director and disseminate the information as necessary to the appropriate Center authorities.

(3) Maintain and centrally control the NASA CI Investigative Management System (NCIMS) for NASA CI/CT inquiries and investigations (except for Office of the Inspector General records). NASA CI/CT inquiries and investigations are conducted to prove or disprove allegations of espionage or other intelligence activities, such as sabotage, assassination, or other national security crimes on behalf of a person, organization, foreign government, or international terrorists affecting NASA. NASA CI/CT inquiries and investigations may establish the elements of proof for administrative actions, provide basis for CI/CT operations, refer information to the Federal Bureau of Investigations (FBI), or validate the suitability of personnel for access to classified information. The CI/CT Program Director or his designee shall approve the initiation and closure of NASA CI/CT inquiries, investigations, and operations.

(4) Be the focal point for making referrals to the FBI pursuant to Section 811 of the Intelligence Authorization Act of 1995 [50 U.S.C. 402 (a)]. Cooperation and contact with the FBI shall be governed by the Memorandum of Understanding between the FBI and NASA, dated December 12, 2002.

(5) Direct HQ and Center CI/CT offices to conduct informative CI/CT Awareness Briefings for NASA Federal and contract employees. The objective of the Awareness Program is to educate and inform NASA audiences and activities (including programs, projects, and operations) about threats posed by FIS, terrorism, and other sources who attempt to obtain NASA information and technology by unauthorized means and provide information on how to

counter such threats.

(6) Coordinate with the OSPP Safeguards Division to obtain CI/CT analysis support and services.

(7) Identify NASA programs or operations having potential for tailored CI/CT support.

(8) Coordinate CI/CT issues with the NASA Chief Information Officer, Assistant Administrator for External Relations, Office of the General Counsel, and other NASA officials as necessary. NASA HQ CI program management shall coordinate with the NASA Inspector General on open CI/CT cases with potential criminal liability, in accordance with NPD 9800.1, at paragraph 5.e.(1).

(9) In order to ensure enhanced security of CI/CT files and records, establish procedural requirements that supplement those of NPR 1441.1, NASA Records Retention Schedules, for the maintenance, retention, and disposition of NASA CI/CT investigative files and records.

b. All NASA Federal and contract employees, organizations, other Federal personnel or military detailees, grantee, or other entity as provided in the governing agreement or instrument and who are located at any NASA installation shall cooperate fully with NASA CI/CT special agents to the extent permitted by law. During the conduct of CI/CT activities, such cooperation shall include the following:

(1) Access to NASA premises, employees, files, and documents (to include hardcopy and electronic) at all NASA locations.

(2) Oral and written statements, including statements under oath or affirmation that are administered by authorized personnel.

(3) Technical consultation, examination, and any other assistance as required.

c. NASA Center Directors are responsible for the following:

(1) Assure NASA Federal and contract personnel under their control comply with this directive.

(2) Maintain office space and provide basic IT and communication support services for CI/CT special agents assigned to their Centers.

(3) Assure that allegations of espionage, terrorism threats, or loss of NASA information or national security information under NASA control are reported to the Center CI office immediately.

(4) Assure that Center and Component Facility personnel attend CI/CT awareness, threat, and foreign travel briefings.

d. Any NASA Federal or contract employee who observes or becomes aware of the deliberate or suspected compromise of information identified in paragraph 1b of this directive shall report such information immediately and in person to their HQ or Center CI office. Any NASA Federal or contractor employee who becomes aware of information pertaining to international or domestic terrorist activities shall report such information immediately and in person to their HQ or Center CI office. If the information indicates a computer compromise or other cyber intrusion, the OIG shall be promptly notified.

6. DELEGATION OF AUTHORITY

None.

7. MEASUREMENTS

The AA shall provide an annual report providing metrics and other information concerning the results of CI/CT inquiries and investigations, terrorism analysis threats, liaison contacts, "Section 811" referrals, and foreign traveler debriefs to the NASA Administrator.

8. CANCELLATION

NPD 1660.1A dated Feb 27, 2002.

/s/ Michael D. Griffin
Administrator

ATTACHMENT A: (TEXT)

None.

(URL for Graphic)

None.

DISTRIBUTION:
NODIS